

PCT

世界知的所有権機関
国際事務局

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類 ³ G05B 9/03, G06F 11/18	A1	(11) 国際公開番号 WO 88/ 04071 (43) 国際公開日 1988年6月2日 (02.06.88)
(21) 国際出願番号 PCT / JP84 / 00251 (22) 国際出願日 1984年5月18日 (18.05.84) (31) 優先権主張番号 特願昭58-85803 (32) 優先日 1983年5月18日 (18.05.83) (33) 優先権主張国 JP (71) 出願人 ; および (72) 発明者 浅見一夫 (ASAMI, Kazuo) [JP / JP] 〒316 茨城県日立市中丸町1丁目26番3号 Ibaraki, (JP) (74) 代理人 弁理士 高橋明夫 (TAKAHASHI, Akio) 〒100 東京都千代田区丸の内1丁目5番1号 株式会社 日立製作所 特許部内 Tokyo, (JP) (81) 指定国 US. 添付公開書類 国際調査報告書 条約64 (3) (ii) に規定された国際出願に基づく特許の公開 (米国特許商標局により1987年5月19日 (19.05.87) に一連番号 4,667,284号として発行された) に従って発行された。		

(54) Title: MULTIPLEX CONTROL APPARATUS

(54) 発明の名称 多重化制御装置

 INPUT SIGNAL CONTROLLER
 CHANGEOVER UNIT A

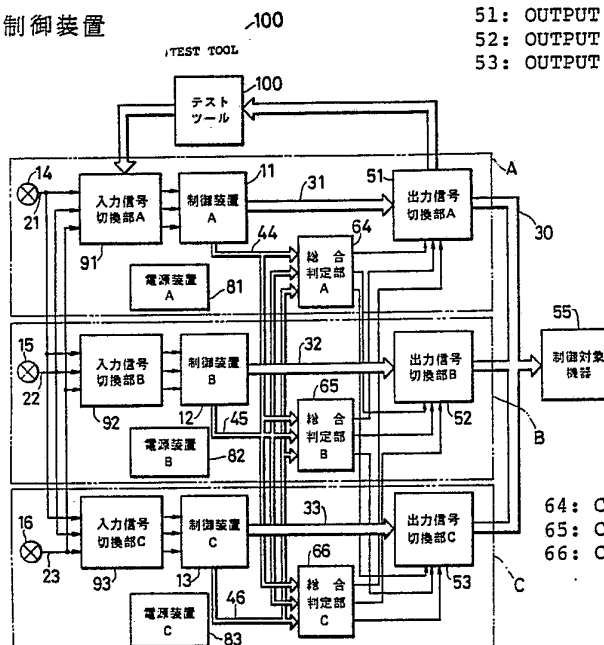
91' POWER SUPPLY A 81

 INPUT SIGNAL CONTROLLER
 CHANGEOVER UNIT B

92' 12' POWER SUPPLY B 82

 INPUT SIGNAL CONTROLLER
 CHANGEOVER UNIT C

93' 13' POWER SUPPLY C 83


 51: OUTPUT SIGNAL CHANGEOVER UNIT A
 52: OUTPUT SIGNAL CHANGEOVER UNIT B
 53: OUTPUT SIGNAL CHANGEOVER UNIT C

 64: COMPOSITE JUDGEMENT UNIT A
 65: COMPOSITE JUDGEMENT UNIT B
 66: COMPOSITE JUDGEMENT UNIT C

(57) Abstract

A highly-reliable multiplex control apparatus is composed of a plurality of subsystems which are completely separate from each other. Signals from status quantity detectors (14, 15, 16) of each of the subsystems are each output to output signal changeover units (51, 52, 53), respectively, through controllers (11, 12, 13) of the subsystems. The controllers (11, 12, 13) diagnose whether the corresponding subsystems are normal or abnormal by self-diagnosis and mutual diagnosis, and output normality judgement signals (44, 45, 46), respectively, indicating the degree of normality thereof. Composite judgement units (64, 65, 66) select the controller which is functioning the most normally on the basis of the normality judgement signals from the controllers. The output signal changeover units (51, 52, 53) select the output of the controller which has the highest degree of normality in accordance with the outputs of the composite judgement units, and deliver the output of that selected controller to a device (55) being controlled.

(57) 要約

完全に分離した複数個のサブシステムよりなる信頼性が高い多重化制御装置。各サブシステムの状態量検出器（14,15,16）からの信号は各サブシステムの制御装置（11,12,13）を介して各出力信号切換部（51, 52,53）に出力される。また、各制御装置（11,12,13）は自己診断・相互診断により各サブシステムの異常を診断し正常性判定信号（44,45, 46）を出力する。総合判定部（64,65,66）は制御装置からの正常性判定信号に基づき最も正常に機能している1つの制御装置を選択する。出力信号切換部（51,52,53）は総合判定部の出力により最も正常に機能している制御装置の出力を選定し制御対象機器55に出力する。

情報としての用途のみ

PCTに基づいて公開される国際出願のパンフレット第1頁にPCT加盟国を同定するために使用されるコード

AT	オーストリア	FR	フランス	MR	モーリタニア
AU	オーストラリア	GA	ガボン	MF	マラウイ
BB	バルバドス	GB	イギリス	NL	オランダ
BE	ベルギー	HU	ハンガリー	NO	ノルウェー
BG	ブルガリア	IT	イタリア	RO	ルーマニア
BJ	ベナン	JP	日本	SD	スーダン
BR	ブラジル	KP	朝鮮民主主義人民共和国	SE	スウェーデン
CF	中央アフリカ共和国	KR	大韓民国	SN	セネガル
CG	コンゴ	LI	リヒテンシュタイン	SU	ソビエト連邦
CH	スイス	LK	スリランカ	TD	チャード
CN	カメルーン	LU	ルクセンブルグ	TG	トーゴ
DE	西ドイツ	MC	モナコ	US	米国
DK	デンマーク	MG	マダガスカル		
FI	フィンランド	ML	マリ		

(1)

明 細 書

多重化制御装置

技術分野

本発明は、多重化制御装置に関する。

5 背景技術

制御装置の高信頼化には種々の方法がある。従来からとられている最も一般的な方法は、制御装置に使用されているハードウェア個々のレベルでの高信頼化である。具体的には、高信頼度部品の選択使用及び、十分な設計
10 裕度の確保、或いは、部品のスクリーニング実施及びエージング実施、さらには使用部品点数の削減（集積回路の適用）などである。しかしながら、これらハードウェアレベルでの高信頼化には限界がある。そこで、最近は、システムレベルでの高信頼化の必要性和有効性が強く認識
15 されてきている。

例えば、従来のシングル系の制御装置のシステム構成では、コンデンサ 1 個又はトランジスタ 1 個の異常が、制御システム全体に大きな影響を与える可能性がある。事実、過去の制御システムの異常原因を分析してみると、
20 ほとんどがこの種のトラブルに起因している。そこで、制御システムを多重化することが考えられている。

制御システムの多重化制御装置は例えば

TRANSACTIONS OF THE AMERICAN NUCLEAR

(2)

- SOCIETY AND THE EUROPEAN NUCLEAR
SOCIETY 1980 INTERNATIONAL
CONFERENCE ON WORLD NUCLEAR ENERGY-
ACCOMPLISHMENTS AND PERSPECTIVES ,
5 Volume 3 5 , 4 0 6 ~ 4 1 1 頁に記載された論文
“ BWR PLANTS IN JAPAN - A NEW
PERSPECTIVE ” 中の 3 . Toshiba BWR Power
Control System ADMIX with Tripple -
Control Channel and self-Diagnoses の FIG.
10 1 に示されている。この FIG. 1 には中間値選択三重化
プラント制御装置の一例が開示されている。即ち、この
三重化プラント制御装置では、フィードバック信号とし
て制御に使用するプロセス信号の reactor water
level, feedwater flow, main steam flow は各々
15 三重化され、各々の信号は 3 信号のうちの中間値を選択
して出力する中間値選択回路 M V G に入力される。中間
値選択回路 M V G により選択された信号は三重化された
master controller M / C に入力される。各 M / C
により演算された 3 つの出力信号の中間値を中間値選択
20 回路 M V G に入力し、この出力が secondary
controller S / C に入力される。この中間値選択回
路 M V G は、例えば高値入力選択回路と低値入力選択回
路の組合せにより作られる。



(3)

しかし、本方式では中間値選択回路の故障がコモンモードとなるので、中間値選択回路 M V G を十分信頼性の高いものにしないと効果は半減する。なお、電源まで含めた多重化を考慮した場合は、この中間値選択回路の電源異常で、三重化プラント制御装置全体が異常となる。

5 なお、制御装置の出力が多数ある場合、本方式では、各出力信号毎に中間値をとる形になるので、制御対象システムによつては、各々の制御装置が干渉しあい、ハンチング現象が発生する可能性がある。

10 発明の開示

本発明の目的は信頼性の高い多重化制御装置を提供することにある。

本発明は、以下に述べる詳細な説明を参照すれば明らかのようにシステム構成面からは、万一の故障発生時にはその故障をマスクし、その故障した機能を代行させるための多重化構成と、万一の故障発生時の危険を最小化するための分散化構成とを合わせた、いわば多重分散化システム構成とすることにより上記の目的を達成するものである。

15

20 図面の簡単な説明

第 1 図は本発明の好適な一実施例である三重化プラント制御装置の系統図、第 2 図は第 1 図に示す各サブシステムにおける制御装置の信号入力側における信号伝送回



(4)

路の系統図、第 3 図は第 1 図に示す各サブシステムの制御装置間における情報伝送回路の系統図、第 4 図は第 1 図に示す各サブシステムにおける制御装置の信号出力側における信号伝送回路の系統図、第 5 図は第 4 図の他の変形例図である。

5 発明を実施するための最良の形態

第 1 図を参照するに、本実施例の三重化プラント制御装置は、完全に分離独立した 3 つのサブシステム A, B, および C からなっている。

10 この三重化プラント制御装置のサブシステム A, B, および C は三重化された検出器 14, 15, 16, 各検出器からの検出信号を入力する入力信号切換部 91, 92, 93, 入力信号切換部からの信号により制御信号を出力する制御装置 11, 12, 13, 制御装置からの
15 信号により最も正常と考えられる 1 つの制御装置を選択するための総合判定部 64, 65, 66, 総合判定部からの選択指令信号により選択された制御装置からの出力信号を制御対象機器に出力させるための出力信号切換部 51, 52, 53, ならびに各サブシステム A, B, C
20 の専用電源装置 81, 82, 83 からなっておりこれらサブシステム A, B, C は以下の詳細な説明で述べるような特徴を具備する。ここでテストツール 100 は各サブシステム A, B, C の回路のチェックを行うために供



(5)

される。

本実施例の三重化プラント制御装置は後述するように、
万一、1つのサブシステム内で異常が発生すると、その
異常部分が属する異常サブシステム内の制御装置 1 1 ,
5 1 2 , 1 3 自体による自己診断機能により検出され、異
常サブシステムを、他の正常なサブシステムから切り離
す。万一、異常サブシステムの自己診断機能により異常
を検出できなかつたとしても、その異常は相互診断機能
により検出されるため他の正常なサブシステムにその影
10 響を及ぼすことはなく、またその異常に基づく現象は異
常サブシステム内に封じ込めることができる。

以下、各サブシステム内の主要構成要素とその動作に
つき説明する。

1) サブシステムへの電源供給

15 各サブシステムは、各々独立した電源装置 8 1 , 8 2
及び 8 3 を所有している。万一あるサブシステム、例え
ばサブシステム A 内の電源装置 8 1 に異常が発生した場
合には、それにより、サブシステム A は、三重化プラ
ント制御装置から切離される。このため、サブシステム A
20 の出力が他のサブシステム B 及び C に影響を与えること
は原理的にない。あえてあるとすれば、後述する情報入
力部において、1 チャンネル分の入力信号が喪失する程
度である。



(6)

2) プラント情報入力方法

本三重化プラント制御装置は、信号の入力系統そのものも多重化することを原則としている。即ち、三重化プラント制御装置は、プラント情報をベースに出力信号を決定するいわば情報処理装置である。従つて、入力情報が単一の場合には、この異常時にその使命が完遂できなくなると考えられるからである。本実施例では、プラントの同じ状態量を測定する検出器が3個設けられる。すなわち、同じ状態量を測定する3個の検出器14, 15及び16が、プラントに設けられる。すべての検出器を三重化するとシステムが複雑になるので、三重化する検出器は、プラントの運転制御にとつて重要なものだけでよい。

さて、本実施例では検出器14, 15及び16の出力信号、すなわち、プラント情報21, 22, 23(制御対象からのフィードバック信号など)は、原則として三重化されている。それらの入力情報は、基本的には各々のサブシステムの入力信号切換部91, 92及び93を介して制御装置11, 12及び13にそれぞれ入力される。また、圧力発信器などの外部電源を必要とする検出器に対しては、それが属するサブシステムの電源装置より電力が供給される。従つて、1つのサブシステムの電源装置が故障した場合、その電源装置から電力が供給さ

(7)

れている検出器は作動しないが、他の2つの検出器は正常に作動するので、各々のサブシステムの制御装置は入力情報を確保出来る。このようにプラント情報が完全に喪失することはない。3つの検出器が同時に故障することとは極めて希なことである。次に、これら多重化された信号の各サブシステムへの入力方法につき説明する。

プラントの同一の状態量を検出する三重化された各検出器の出力信号を、各サブシステムに入力する方法としては、第1図に示した如く、各々の検出器から出力されたプラント情報を各サブシステムの全てにそれぞれ入力する方法と、1対1、即ち、その検出器が属するサブシステムのみへ入力する方法（図示せず）の2つがある。両者の使いわけは、主に要求信頼度と経済上の観点から決められる。前者の方法は、単純に言つて後者の方法の3倍のプラント情報を入力することになり、入力部及びその入力信号の処理部が増大する。現実的には、プラントの制御上特に重要な信号は、前者の方法とし、各サブシステム内で、各々の多重化信号をチェックし、最も真値に近いと考えられる信号を選択、或いは算出し、自己の演算用データとしている。これは、プラントに設けられた検出器の異常による悪影響をサブシステムにできる限り及ぼさないようにするためである。

3) 入力信号の分離と切離し



(8)

各検出器 14, 15 及び 16 にて検出されたプラント
情報は、入力信号切換部 91, 92 及び 93 を介し、制
御装置 11, 12, 13 に入力する。入力信号切換部
91, 92, 93 は、本実施例では具体的には電磁リレ
5 ー、水銀リレーなどによつて構成されている。しかし、
必ずしもこの種のハードウェアによるものでなくてもよ
い。

万一、1つのサブシステム内に異常が発生した場合
(例えば電源装置の異常、制御装置の異常など)、その
10 異常サブシステムは、該当する入力信号切換部及び出力
信号切換部(後述)により、制御対象機器及びプラント
1 から完全に切離される。

また、切離された異常サブシステムのトラブルシュー
ティング及び修復後の動作確認を容易にするために、入
15 力信号切換部 91, 92, 93 及び出力信号切換部 51,
52, 53 は、テストツール 100 からの信号を入力で
きるように構成されている。この機能は、後述の第2図
に示されたりレーの接点U側にテストツール 100 から
の信号を入力することにより実現している。なお、テス
20 トツール 100 は図示してない信号入力部、信号演算部、
ならびに信号発生部を有する。

サブシステム A に属する検出器 14 の出力信号を、各
各のサブシステムに設けられる制御装置 11, 12 及び



(9)

1 3 に伝える具体的な信号伝送回路を第 2 図に示す。検
出器 1 4 への電力は、サブシステム A 内の電源装置 8 1
より供給されている。電源ライン（2 線式検出器を例に
とっており、信号ラインに一致）には、ヒューズ 2 5 A、
5 スイッチ 2 4 A 及びリレー 2 6 A が接続されている。ヒ
ューズ 2 5 A は、信号伝送回路の保護用である。スイッ
チ 2 4 A は、万一、検出器 1 4 に異常が発生した時のメ
インテナンス時に、検出器 1 4 を電源装置 8 1 及び各制
御装置から切離せるように設置してある。またリレー
10 2 6 A は、検出器 1 4 への供給電力を監視するものであ
る。スイッチ 2 4 A の動作位置及びリレー 2 6 A の接点
状態により、各サブシステムの制御装置がそれぞれに取
り込んだ検出器 1 4 の出力信号が使用可能状態にあるの
か、それとも無視すべき状態にあるのかを判断すること
15 ができる。検出器 1 4 の出力信号（一般には 4 ~ 2 0
mA・DC）は、5 0 Ω 程度の抵抗 2 7 A, 2 8 A 及び
2 9 A により、電圧信号に変換される。この電圧信号が、
入力信号切換部（水銀リレー）9 1, 9 2 及び 9 3 の接
点を介して各制御装置 1 1, 1 2 及び 1 3 にそれぞれ入
20 力されている。この場合、入力信号切換部 9 1, 9 2 及
び 9 3 の接点 V と接点 W が、それぞれ接続されている。

検出器 1 5 及び 1 6 も、第 2 図と同様な信号伝送回路
に接続されている。検出器 1 5 及び 1 6 の出力信号は、



(10)

上記信号伝送回路を介して制御装置 1 1, 1 2 及び 1 3 にそれぞれ伝えられる。

制御装置 1 1, 1 2 及び 1 3 の入力回路方式によれば、その入力インピーダンスは電源が入っているときには各
5 各 1 0 ~ 1 0 0 M Ω 程度、電源が入っていないときには数 K Ω 程度以下に低下することがある。このような信号伝送回路を用いると、各システム毎に小さな抵抗 2 7 A, 2 8 A、ならびに 2 9 A が直列に入っているので、あるサブシステム内で制御装置 1 1, 1 2、又は 1 3 の短絡、
10 地絡、又は内部インピーダンスの変化などのトラブルが発生したとしても、他のサブシステムに対する入力信号（プラント情報）に影響を与えることはほとんどない。
なお、入力信号切換部 9 1, 9 2 及び 9 3 の接点 U は、テストツール 1 0 0 の接続用コネクタ（図示せず）に接
15 続されている。あるサブシステムに異常が生じた場合は、異常サブシステムの入力信号切換部の接点 V と接点 W の接続を切離し、その後、接点 U と接点 W を接続する。テストツール 1 0 0 から出力された検出器の出力信号に相当する模擬信号が、接点 U 及び W を介して異常サブシ
20 テムの制御装置に入力される。この制御装置に、テストツール 1 0 0 の出力信号を入力することによつて各サブシステム毎の種々のテストが行われる。

4) 制御装置の機能と出力信号



(11)

- 各サブシステムの制御装置 1 1 , 1 2 及び 1 3 は、入力信号切換部 9 1 , 9 2 , 9 3 を介し入力したプラント情報 2 1 , 2 2 及び 2 3 に基づいて得られた制御信号 3 1 , 3 2 及び 3 3 をそれぞれ出力する。但しテストツール 1 0 0 が接続されている制御装置のテスト中は、テストツール 1 0 0 の出力モードに対応した信号を出力する。また、各々の制御装置は、それらが属する当該サブシステムの制御装置 1 1 , 1 2 , 1 3 自体が内蔵するパリティチェックなどの自己診断のほかに、後述の第 3 図
- 10 に示す情報伝送回路を介して入力される他のサブシステムからの入力を使用して各制御装置 1 1 , 1 2 , 1 3 内で実施される相互診断により、サブシステム異常の早期発見ができるとともに、これらの結果から制御対象機器 5 5 に対し制御信号 3 1 , 3 2 , 3 3 の何れから制御対象機器 5 5 へ入力するかを決定している。すなわち必ずしも自己のサブシステムのデータを常に出力するわけではなく、診断結果を尊重し、その時点で最も妥当と考えられる多数決の原理により決定されたデータ制御対象機器に出力する。
- 20 本来、共通部の最少化という観点からは、各サブシステム間同士の信号の相互授受はないほうがよいし、多重分散化の思想にも合致する。しかしながら、サブシステム間での切換時のバンプレス性や、異常復帰後のサブシ



(12)

システム再立ち上げ時などの内部データ設定機能などの確保のためには、若干のデータの授受が必要不可欠となる。特に、制御演算として、比例積分制御あるいはラッチデータなど、過去の履歴を必要とするデータを扱う場合には、ある種のデータコピー機能が必要となる。また、確

5 実な異常検出のためには、自己のデータ以外の他のデータを入手し、これらの相互比較を行なうことも必要となる。しかしながら上記した様に、本機能は、共通モード故障をひきおこす可能性もあるのでその適用には十分な

10 注意が必要である。本実施例では、第3図に示すように信頼性の高いデータ伝送装置回路34, 35及び36と、伝送回路切離装置37, 38及び39の適用に加え、データの二重伝送方式と、各サブシステム毎のデータコントロール方式により、本機能のコモンモード化を極力防

15 止している。第3図により以下本機能のコモンモード化防止について説明する。なお第3図における制御装置11, 12ならびに13は第1図における制御装置11, 12ならびに13に対応する。

データ伝送回路34, 35及び36は、光伝送技術を

20 応用した絶縁型データ伝送回路を使用している。第3図においてデータ伝送回路34, 35及び36がそれぞれ2本ずつ示されているが、これは制御装置11, 12ならびに13間のデータの流れをわかりやすくしたためで

(13)

ある。実際は、データ伝送回路 3 4 , 3 5 及び 3 6 は、一本であつてもよい。データ伝送回路 3 4 は、制御装置 1 1 と制御装置 1 2 を接続している。データ伝送回路 3 5 は、制御装置 1 2 と制御装置 1 3 を連絡している。

5 データ伝送回路 3 6 は、制御装置 1 1 と制御装置 1 3 を連絡している。1つのデータ伝送回路は、それによつて連絡される一方の制御装置内のデータを他方の制御装置に伝える。そのデータ伝送回路は、逆に、他方の制御装置内のデータを一方の制御装置に伝える。このため、サブシステム A の制御装置 1 1 内のサブシステム A に関するデータは、データ伝送回路 3 6 を介してサブシステム C の制御装置 1 3 に伝えられ、さらにそこからデータ伝送回路 3 5 を介してサブシステム B の制御装置 1 2 に伝えられる。逆に、制御装置 1 1 内のサブシステム A に関するデータは、データ伝送回路 3 4 を介して制御装置 1 2 に伝えられ、さらにそこからデータ伝送路 3 5 を介して制御装置 1 3 に伝えられる。制御装置 1 2 内のサブシステム B に関するデータ及び制御装置 1 3 内のサブシステム C に関するデータも、前述のサブシステム A に関するデータと同様に各々のデータ伝送回路を介して他の制御装置に伝えられる。1つの制御装置は、自己のデータと、異なるデータ伝送回路によつて伝えられた他の2つの制御装置のデータを2種類ずつ、合計5種類のデー



(14)

タを所有している。

伝送回路切離し装置 3 7 が、データ伝送回路 3 4 に設けられる。伝送回路切離し装置 3 8 が、データ伝送回路 3 5 に設けられる。伝送回路切離し装置 3 9 が、データ
5 伝送装置 3 6 に設置される。

もし、データ伝送回路 3 4 , 3 5 及び 3 6 の 1 つに異常が発生した場合、または制御装置 1 1 , 1 2 及び 1 3 の 1 つに異常が発生したことを自己診断あるいは自己の制御装置内のデータと他のサブシステムの制御装置から
10 データ伝送回路 3 4 , 3 5 , 3 6 を介して自己の制御装置に入力したデータと比較することにより実施される。
いわゆる相互診断により検出した場合は、その異常箇所
に該当する伝送回路切離し装置を作動させて異常箇所を
正常な部分から切離す。これによつて、コモンモード故
15 障を阻止できる。各データ伝送回路は、前述したように
それが接続される制御装置から出力されたデータとともに
に他の伝送回路を介して入手した他の制御装置のデータ
をのせて伝送しあう二重伝送方式を採用しているので、
1 つのデータ伝送回路が異常になつた場合でも、それぞ
20 れの制御装置に異なる他のすべての制御装置のデータを
入力することができる。

本実施例では、このように二重伝送方式を採用することにより各制御装置の相互間を連絡するデータ伝送回路



(15)

は単一でありながらデータ伝送に関しては二重化された信頼性の高いデータ伝送方式を実現している。

制御装置 11, 12 及び 13 は、前述のように各データ伝送回路により入手した各サブシステムのデータをベースに相互診断を実施する。基本的には、ビットデータ
5 に対しては 2 out of 3 ロジックを応用した論理により数値データに対しては偏差チェックをベースにした論理により、制御装置 11, 12 及び 13 は出力データを決定する。この決定は、各サブシステムがその時点で所有している各サブシステムのデータに基づいて、各サブシステム
10 の判断により独立して行なう方式としているため、極めてコモンモード故障をひきおこしにくい形となっている。また、制御装置の自己データと、他の制御装置のデータ及び制御装置の出力データとを制御装置内で分離
15 して取扱う方式としている。従つて、万一ある制御装置の自己演算データが他の 2 つのサブシステムのデータと一致しない事象が発生した場合には、制御装置の出力データは、一致している他の 2 つのサブシステムのデータとする。しかし、自己の演算データの変更は、その不一致
20 事象が複数回あるいは一定時間以上連続して発生しない限り行なわない。このように、ある制御装置の自己演算結果とその制御装置からの実際の出力信号とを別個のものとして管理する方式をとることにより、自己データ



(16)

の他のサブシステムのデータからの汚染を防止するとともに、相互診断機能に用いる各サブシステムのデータの独立性を確保している。

制御装置 1 1, 1 2 及び 1 3 で得られたそれぞれの自己診断及び相互診断結果は、第 1 図ならびに第 4 図に示す診断結果信号 4 4, 4 5 及び 4 6 として制御装置 1 1, 1 2 及び 1 3 より総合判定部 6 4, 6 5 及び 6 6 にそれぞれ出力される。1 つの総合判定部には、診断結果信号 4 4, 4 5 及び 4 6 が入力される。本実施例では、各制御装置 1 1, 1 2 及び 1 3 は、各サブシステム毎の正常性を判定し、正常と考えられるサブシステムに対しては「1」、異常と考えられるサブシステムに対しては「0」を出力する。これは後述するように総合判定回路 6 4, 6 5 及び 6 6 の判定ロジックを単純化するためである。すなわち、この総合判定回路は後述の説明により明らかとなるように、制御装置 1 1, 1 2 ならびに 1 3 の内、例えば制御装置 1 1 がフオールしたときに、制御装置 1 2 あるいは 1 3 からの診断結果信号 4 5 あるいは 4 6 のうち、何れの診断結果信号を選択して出力信号切換部 5 1 に出力するかと云うような場合に出力信号切換部 5 1 の制御信号選択切換時間を最小にする上で必要である。

さらに各制御装置においてよりきめ細かな判定を行う



(17)

場合には、各サブシステム毎の状態判定結果を、重故障、中故障、軽故障、正常などと分類し出力させてもよい。また、いわば各サブシステムの正常度などを数値で出力させてもよい。

5 5) 制御信号選択部

本実施例の中核をなすのが、制御信号選択部である。制御信号選択部は、各サブシステム毎に設けられた総合判定部 6 4 , 6 5 及び 6 6 と、各サブシステムの総合判定部 6 4 , 6 5 及び 6 6 の出力により実際に出力信号を
10 切替える出力信号切替部 5 1 , 5 2 及び 5 3 よりなる。出力信号切替部 5 1 , 5 2 及び 5 3 は、プラントの制御対象機器 5 5 に接続されている。

多重化プラント制御装置において最も問題となるのは、いかにして最適な制御信号を選択するかということである。一般の多重化プラント制御装置では、いわゆるポータ部と呼ばれる総合判定部がシングル、すなわち、本実施例のような相互判断方式によらず、1 個のポータ部からの制御信号により各出力信号切替部を操作する方式をとっているため、万一、ポータ部が誤判断すると、多重
15 化プラント制御装置全体の機能の健全性が阻外される可能性があつた。本実施例では、各サブシステム毎に総合判定部 6 4 , 6 5 及び 6 6 を設け、各々の総合判定部の出力信号から 2 out of 3 ロジックに基づいて最も正常
20



(18)

に機能していると思われる制御装置を選択する新たに考えた判定部冗長化方式を採用している。

実際には、総合判定部 6 4 , 6 5 及び 6 6 は 4) 項で述べたように、各制御装置 1 1 , 1 2 及び 1 3 がそれぞれ出力した各サブシステムの診断結果信号 4 4 , 4 5 , 4 6 を全て取り込み、「1」を出力した診断結果、信号の数に基づく多数決判定ロジックによつて最も正常に機能している可能性が高いと推定される 1 つの制御装置を選択し、その旨の選択信号を各々独自に出力する。もし、2 つのサブシステムの制御装置が全く同じ程度に正常に機能していると判断された場合には、総合判定部は、前回から選択されている一方のサブシステムの制御装置を、または両者のうちで優先順位の高いサブシステムの制御装置を選択する。このような場合に備えて、制御装置 1 1 , 1 2 及び 1 3 には、選択する優先順位、例えば、制御装置 1 1 , 1 2 及び 1 3 の順に順位をつけてある。従つて、各総合判定部は、いかなる事態においても判定の時点で最も正常に機能していると思われる制御装置を 1 つだけ選択する。

各々の総合判定部から出力された選択信号は、各出力信号切換部 5 1 , 5 2 及び 5 3 のすべてに入力される。従つて 1 つの出力信号切換部は、3 つの総合判定部 6 4 , 6 5 及び 6 6 からの選択信号を入力することになる。出



(19)

力信号切換部の詳細構造を出力信号切換部 5 1 を例にと
つて第 4 図により説明する。出力信号切換部 5 2 及び
5 3 は、出力信号切換部 5 1 と同一の構成を有する。出
力信号切換部 5 1 は、総合判定部 6 4 , 6 5 及び 6 6 が
5 出力したすべての選択信号を入力する 2 out of 3 ロジ
ック回路 5 4 A、2 つの総合判定部が異常、または動作
不能になつたときに残りの動作中の総合判定部の判定に
従つた結果を出力する 2 out of 3 ロジックバイパス回
路 5 4 B、制御装置から出力された制御信号を入力する
10 固定接点 P、プラント 1 の制御すべき制御対象機器 5 5
に接続される固定接点 Q、固定接点 R 及び可動接点 S か
らなつている。固定接点 R には、必要に応じてテストツ
ール 1 0 0 を接続する。サブシステム A の出力信号切換
部 5 1 に設けられた 2 out of 3 ロジック回路 5 4 は、
15 3 つの総合判定部 6 4 , 6 5 及び 6 6 から出力された 3
つの選択信号のうち 2 以上の選択信号が制御装置 1 1 を
選択したものである場合に、出力信号切換部 5 1 の可動
接点 S を作動させて固定接点 P と固定接点 Q を接続する。

しかしながら、通常の 2 out of 3 回路は、3 つの入
20 力信号のうち 1 つの入力信号の異常をマスクできるが、
2 つの入力信号の異常時は動作できないという欠点を持
つ。そこで本実施例では、各総合判定部 6 4 , 6 5 及び
6 6 に自己診断機能を付加して 2 つの総合判定部で異常



(20)

であるとの自己診断結果がでた時は、残りの総合判定部の判断のみで、制御信号の選択が出来るよう 2 out of 3 ロジックバイパス回路 5 4 B も設けている。

出力信号切換部 5 1 の可動接点 S は、上記の場合以外
5 においては固定接点 S と固定接点 Q を接続しない。サブシステム B の出力信号切換部 5 2 に設けられた 2 out of 3 ロジック回路は、入力された 3 つの選択信号のうち 2 以上の選択信号が制御装置 1 2 を選択したものである場合に、出力信号切換部 5 2 の可動接点 S を作動させてその固定接点 P と固定接点 Q を接続する。また 2 out of 3
10 ロジックバイパスロジック成立時にも可動接点 S を作動させその固定接点 P と固定接点 Q を接続する。

サブシステム C の出力信号切換部 5 3 に設けられた 2 out of 3
15 ロジック回路は、入力された 3 つの選択信号のうち 2 以上の選択信号が制御装置 1 3 を選択したものである場合に、出力信号切換部 5 3 の可動接点 S を作動させてその固定接点 P と固定接点 Q を接続する。また 2 out of 3
20 ロジックバイパスロジック成立時にも可動接点 S を作動させ、その固定接点 P と固定接点 Q を接続する。

従つて、総合判定部 6 4 , 6 5 及び 6 6 の 1 つに異常が発生したとしても、2 out of 3 回路 5 4 A を設けることにより最終的な制御信号の選択が誤まることはない。



(21)

また、出力信号切換部の1つに異常が発生しても問題はない。また、本実施例は、上述のように2 out of 3 ロジックバイパス回路54Bを設けることにより2つのサブシステムが何らかの原因でダウン状態にある時または
5 オフライン状態にある時は、残りのサブシステムで異常であるとの自己診断結果を得ていない場合に限り、自動的にこの残りのサブシステムを選択できるような機能をも有している。これらの機能を有する本実施例は、最終的には3台中1台のみ運転続行可能であれば、制御続行
10 可能なシステムを実現している。

第4図においては、接点P, Q, Rが1個であるため、たとえばリレーなどでこの接点を構成した場合は接触不良、あるいは接点溶着、コイル断線などのリレーの単一故障でたとえ制御装置11が選択されていても、その出力
15 信号は制御対象に伝達されなかつたり、2つ以上の制御装置の出力が制御対象に伝達されたりすることがありうる。一般にリレー等の信頼性は高いので問題になることは少ないが、もしこの部分の単一故障をも防止したいという場合には、上記第4図に示すロジックを直接に出
20 力信号選択ラインにより回路を構成した第5図に示す回路を適用することも可能である。

なお、ちなみに3つのサブシステムが全てダウンした場合には、その出力は、システムの、フェイルセーフ、



(22)

フェイルアブイズなどの方向に動作することはもちろんである。

本実施例によれば、多重化の効果を十分に生かせるため、極めて高信頼度を期待できるフォールトトララントシステムを構築することができる。

以上述べた本実施例によれば、多重化プラント制御装置の信頼性が著しく向上し、プラントの稼働率が著しく向上する。

また、総合判定部の判定ロジックを多数決判定方式として説明したが、よりきめこまかな判定ロジックとして、各サブシステムの状態を重故障，中故障，軽故障，正常などと分類する場合は、それぞれ、最も正常に近いものから順次選択する方法や、各サブシステムの正常度などを数値で表現した場合は、これら数値の最大のシステムを選択する方法なども考えられる。この場合、判定結果そのものはよりきめ細かなものになるが、総合判定部のロジックが複雑になるという欠点も有する。

なお、無用の切換を防止するために、例えば、同ランクだつた場合は、現在制御中として選択されているものをそのまま選択させておくことなどのロジックを入れることも効果がある。

本発明は、三重化プラント制御装置だけでなく二重化プラント制御装置にも適用できる。



(23)

本発明によれば、共通部を最小とした多重化システムを構成できるので、特に高信頼化システムの実現が容易に可能となる。

5

10

15

20



(24)

請求の範囲

1. 状態量を検出する検出器と、前記検出器からの出力信号を入力して演算処理し出力信号を出力するとともに、前記出力信号の正常性ならびに演算装置を含む制御装置の正常性を判定し、前記出力信号ならびに制御装置が正常な場合と異常な場合の各々についてそれぞれ異なる診断結果信号を出力する複数の制御装置と、前記制御装置からの前記診断結果信号に基づき多数決の原理に基づき最も正常に機能している1つの制御装置を選択して、選択された制御装置に対応する選択指令信号を出力する総合判定部と、前記総合判定部からの選択指令信号に基づき最も正常に機能している制御装置からの出力信号を選択して制御対象機器に出力する出力信号切換部とよりなることを特徴とする多重化制御装置。
- 15 2. 第1項記載の多重化制御装置において、前記制御装置はその出力信号ならびに、制御装置の正常性を前記制御装置内の演算器または診断回路による自己診断により判定することを特徴とする多重化制御装置。
- 20 3. 第1項記載の多重化制御装置において、前記制御装置はその出力信号の正常性と、異常性の診断結果信号を出力することを特徴とする多重化制御装置。
4. 第1項記載の多重化制御装置において、前記総合判定部は最も正常に機能している1つの制御装置を選択す



(25)

るに際し、あらかじめ決められた優先順位に基づき正常に機能している制御装置を選択することを特徴とする多重化制御装置。

5 5 . 第 1 項記載の多重化制御装置において、前記制御装置は自己の制御装置の演算情報を他の制御装置に伝送するとともに、他の制御装置の演算情報を自己の制御装置に伝送するため情報伝送回路を有し、各制御装置は前記情報伝送回路を介して自己の制御装置内に入力した他の
10 制御装置からの演算情報と自己の演算情報とを比較して自己の演算結果の正常性および他の制御装置の演算結果の正常性を判定することを特徴とする多重化制御装置。

6 . 第 1 項記載の多重化制御装置において、前記検出器と前記制御装置間に発生した異常信号が前記制御装置に入力するのを防止するための入力信号切換部を設けたこと
15 を特徴とする多重化制御装置。

7 . 第 1 項記載の多重化制御装置において、前記検出器は各制御装置ごとに専用の検出器を設けたことを特徴とする多重化制御装置。

8 . 第 1 項記載の多重化制御装置において、前記出力信号
20 号切換部は全ての総合判定部からの選択指令信号を入力し、同一の値の選択指令信号が少なくとも 2 個あるときには、前記同一の値の選択指令信号に基づき最も正常に機能している 1 つの制御装置からの出力信号を選択して



(26)

前記制御対象機器に出力することを特徴とする多重化制御装置。

9. 第1項記載の多重化制御装置において、前記出力信号切換部は全ての総合判定部からの選択指令信号を入力し、他の総合判定部からの選択指令信号が異常であり、自己の総合判定部の選択指令信号が正常である場合、自己の選択指令信号に基づき自己の制御装置からの出力信号を選択して制御対象機器に出力することを特徴とする多重化制御装置。

10. 第5項記載の多重化制御装置において、前記制御装置は、自己の制御装置の演算情報が他の複数個の制御装置からの演算情報と一致している場合には自己の制御装置の演算情報に基づき出力信号を送出し、自己の制御装置の演算情報が他の複数個の制御装置からの演算情報と複数回あるいは一定時間以上連続して一致しない場合には自己の制御装置の演算情報を一致している他の制御装置の演算情報におきかえて、おきかえられた演算情報に基づき自己の制御装置から出力することを特徴とする多重化制御装置。

11. 第5項記載の多重化制御装置において、さらに前記制御装置が自己の演算結果を異常と判定したときに、異常信号が正常な制御装置に前記情報伝送回路を介して伝送されるのを防止するため前記情報伝送回路に伝送回路



(27)

切離し装置を設けたことを特徴とする多重化制御装置。

12. 第5項記載の多重化制御装置において、前記伝送回路は光伝送を応用した絶縁型データ伝送回路であることを特徴とする多重化制御装置。

- 5 13. 第6項記載の多重化制御装置において、前記入力信号切換部、前記制御装置、前記総合判定部、ならびに前記出力信号切換部は同一の制御対象システムを制御するための複数のサブシステムによつて構成され、前記サブシステムは各々個々に電源を具備することを特徴とする
- 10 多重化制御装置。

14. 第6項記載の多重化制御装置において、前記入力信号切換部ならびに前記出力信号切換部は前記検出部ならびに前記制御装置からの入力信号をそれぞれしや断状態に依持するための中間端子を有し、テストツールの信号
- 15 発生部からの出力信号を前記中間端子間に印加することにより前記個々のサブシステムをテストするためテストツールを具備することを特徴とする多重化制御装置。

15. 同一の制御対象システムを制御するために下記よりなるサブシステムを複数個組合せることにより構成される
- 20 多重化制御装置、

- (1) 同一状態量を検出するために各サブシステム毎に設けられる検出器、
- (2) 前記検出器から異常信号が自己のサブシステムに



(28)

入力するのをしや断するための入力信号切換部、

(3) 前記入力信号切換部を介して入力される前記検出器からの信号をもとに出力信号を演算して出力する制御装置、前記制御装置は自己のサブシステムの制御装置

5 置の演算結果を他のサブシステムの制御装置に伝送するとともに他のサブシステムの制御装置の演算結果を自己のサブシステムの制御装置に伝送するための情報伝送回路を有し、各サブシステムの制御装置は前記情報伝送回路を介して自己のサブシステムの制御装置に
10 入力される他のサブシステムの制御装置からの演算結果と自己のサブシステムの演算結果とを比較して自己および他のサブシステムの制御装置からの演算結果の正常性を判定し、自己のサブシステムの制御装置の演算結果が正常な場合と異常な場合の各々についてそれ
15 ぞれ異なる診断結果信号を出力する、

(4) 前記制御装置が自己のサブシステムの制御装置の動作状態を異常と判定したときに異常情報が正常な制御装置に前記情報伝送回路を介して伝送されるのをし
20 や断するために前記データ伝送回路に設けられる伝送回路切離し装置、

(5) 前記制御装置からの前記診断結果信号に基づき最も正常に機能している1つの制御装置に対応する選択指令信号をあらかじめ決められた優先順位に従つて選



(29)

択して出力するための総合判定部、

(6) 前記総合判定部からの選択指令信号に基づき最も
正常に機能している制御装置からの出力信号を選択し
て制御対象機器に出力する出力信号切換部。

5

10

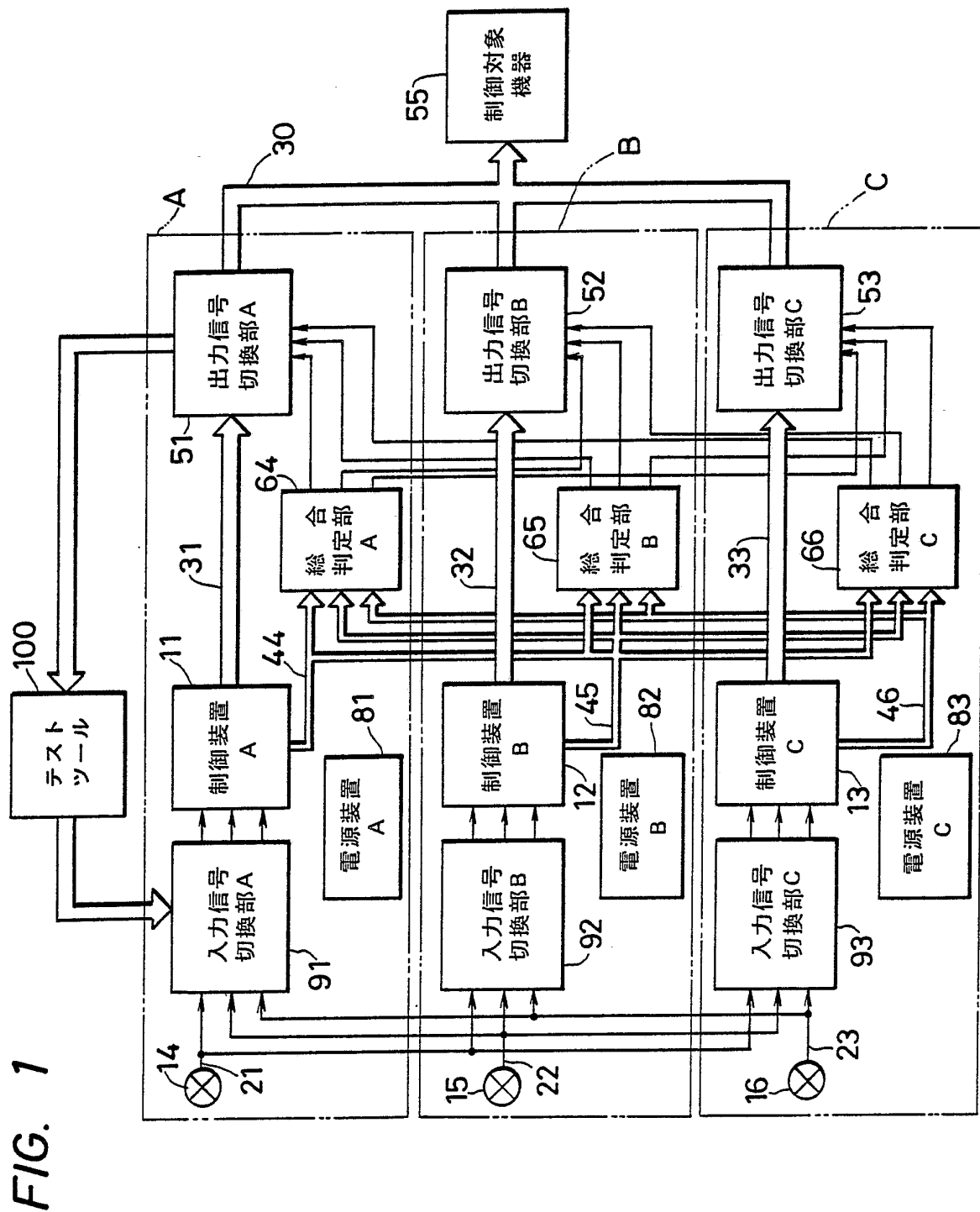
15

20



1/5

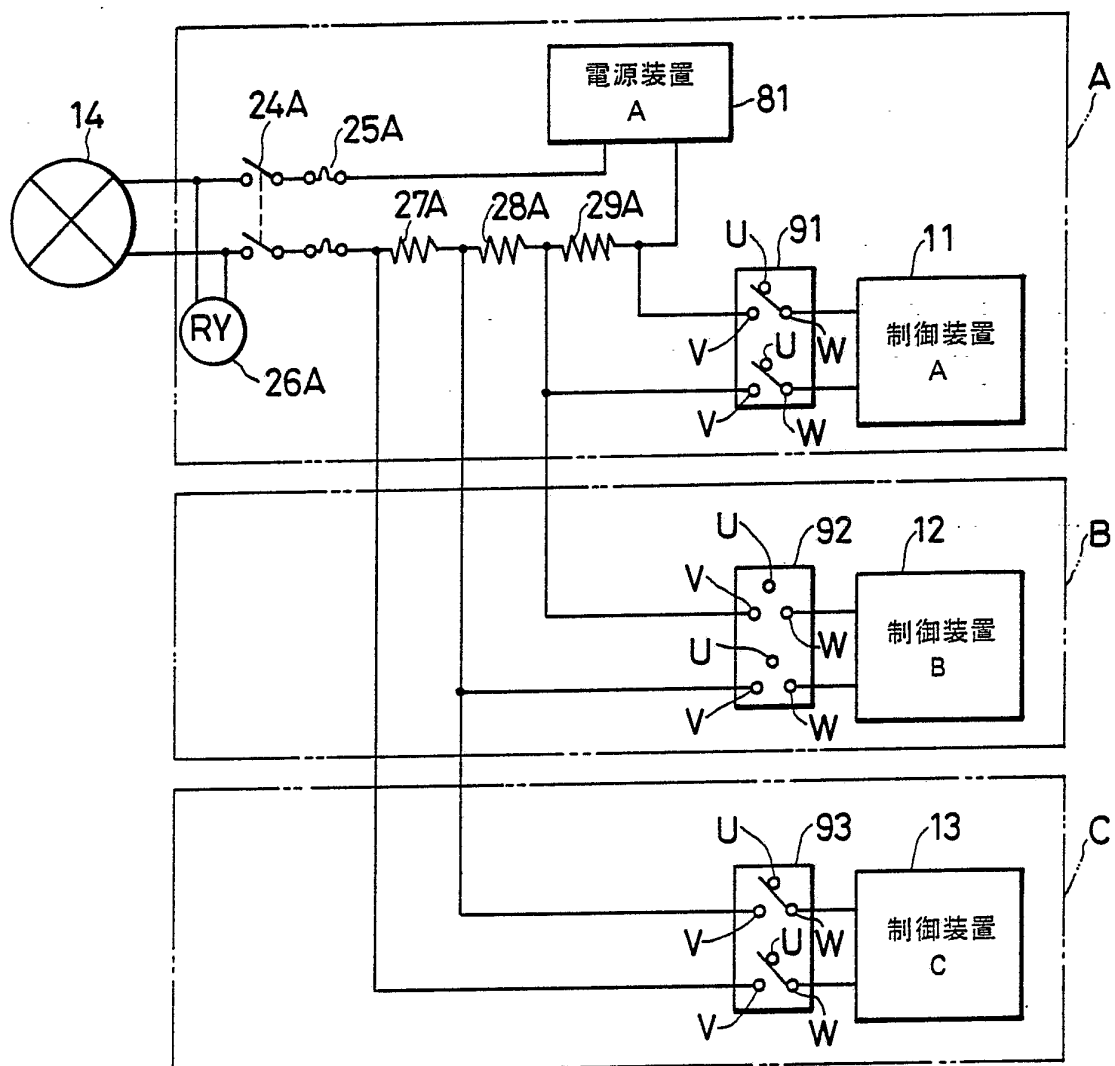
(1)



2/5

(2)

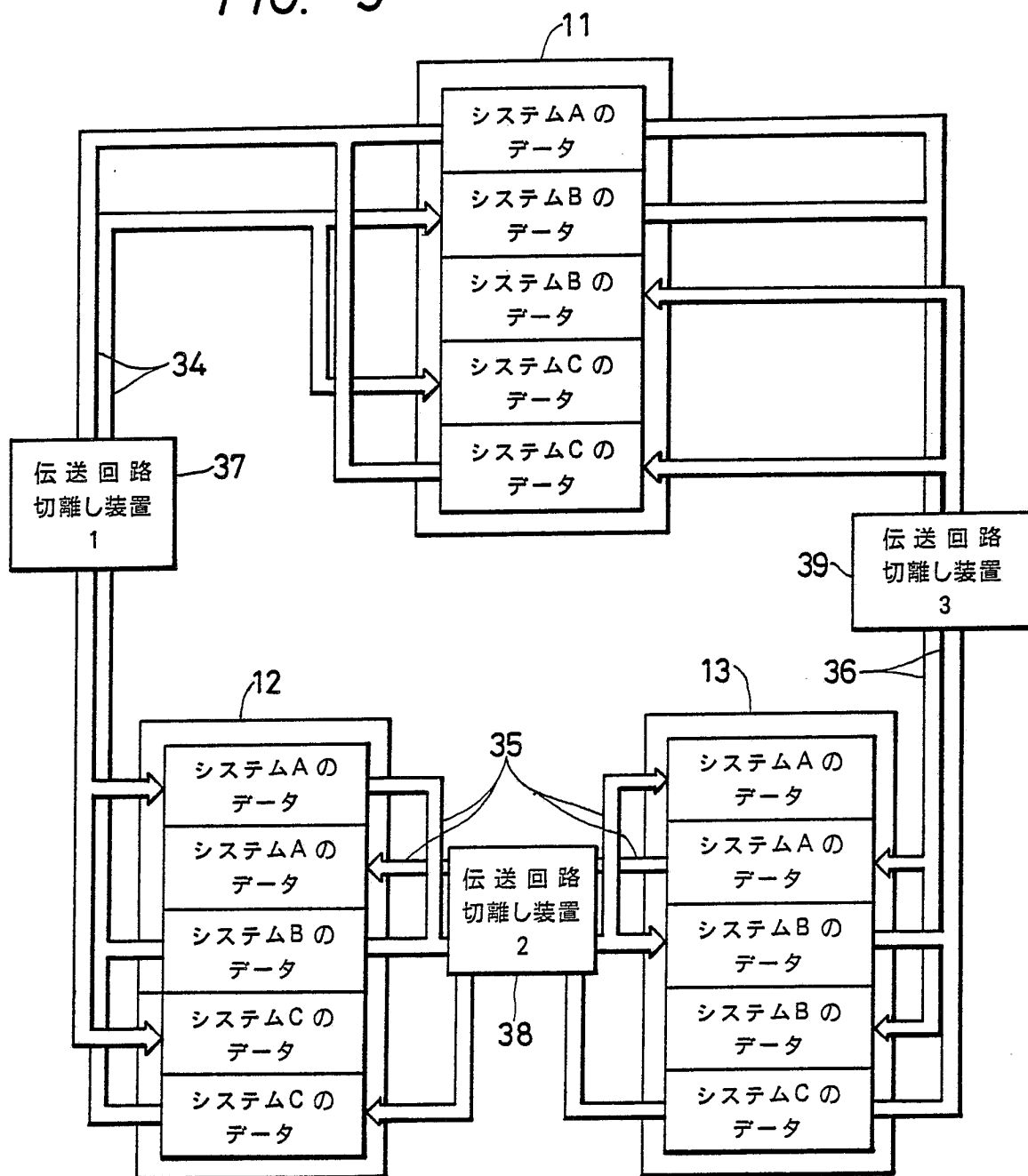
FIG. 2



3/5

(3)

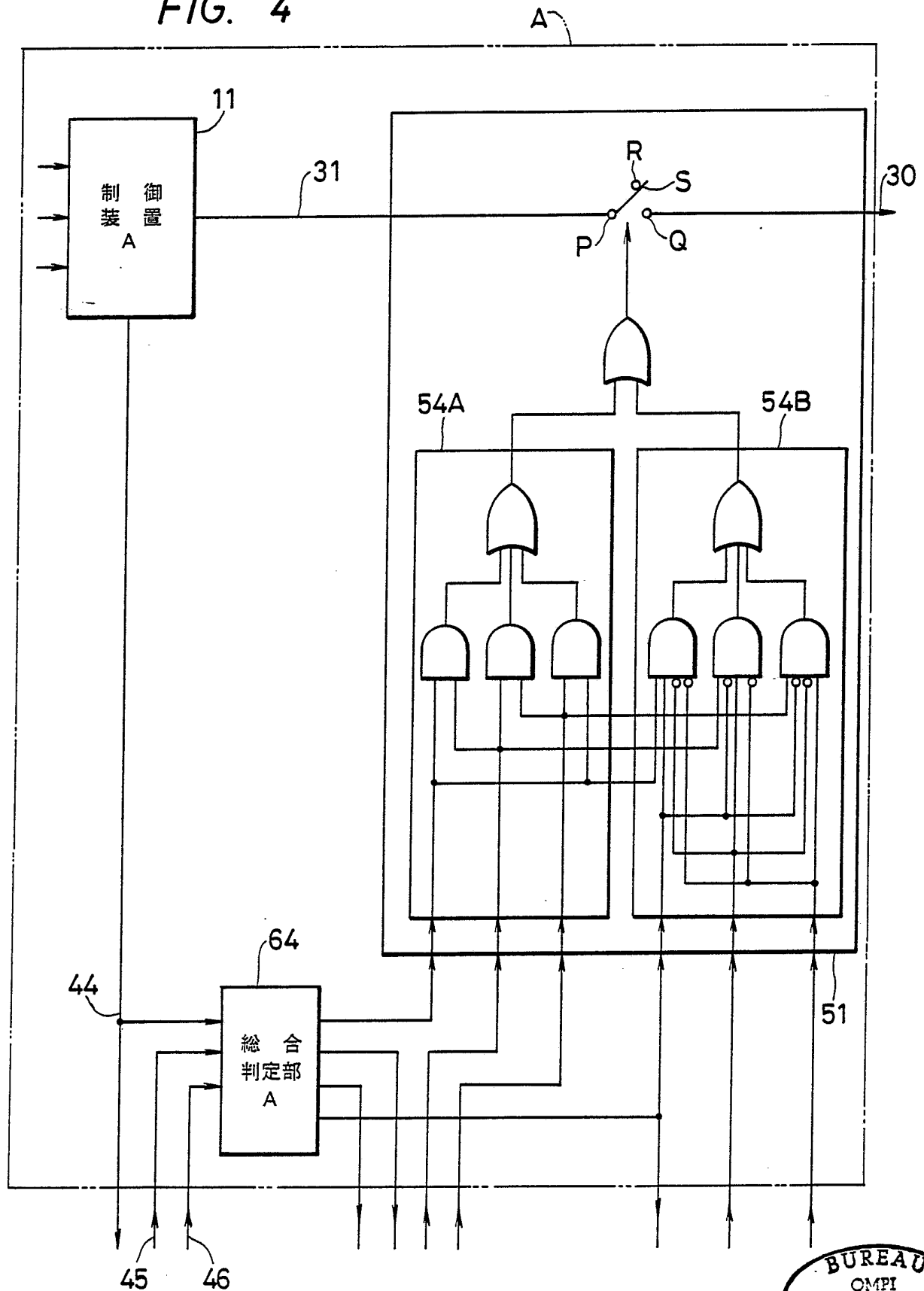
FIG. 3



4/5

(4)

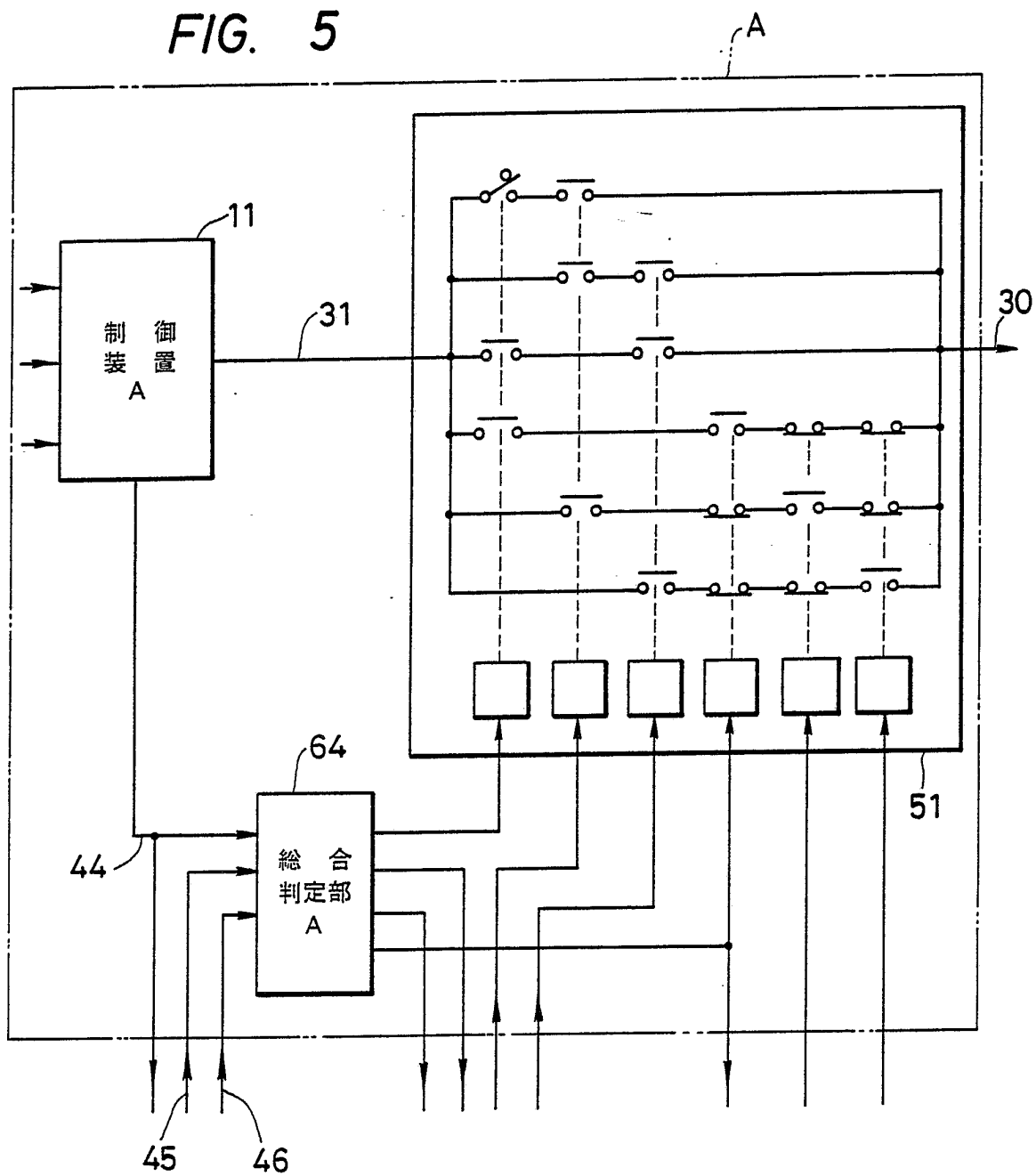
FIG. 4



5/5

(5)

FIG. 5



INTERNATIONAL SEARCH REPORT

International Application No. PCT/JP84/00251

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ³		
According to International Patent Classification (IPC) or to both National Classification and IPC		
Int. Cl. ³ G05B 9/03, G06F 11/18		
II. FIELDS SEARCHED		
Minimum Documentation Searched ⁴		
Classification System	Classification Symbols	
IPC	G05B 7/00-7/02, G05B 9/00-9/03, G05B 23/00-23/02, G06F 11/18	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁵		
Jitsuyo Shinan Koho	1926 - 1984	
Kokai Jitsuyo Shinan Koho	1971 - 1984	
III. DOCUMENTS CONSIDERED TO BE RELEVANT ¹⁴		
Category ^a	Citation of Document, ¹⁶ with indication, where appropriate, of the relevant passages ¹⁷	Relevant to Claim No. ¹⁸
Y	JP, A, 58-37702 (Hitachi, Ltd.) 3 May 1983 (03. 05. 83)	1 - 15
Y	JP, A, 48-61886 (Hitachi, Ltd.) 29 August 1973 (29. 08. 73) & DE, B2, 2258917 & CA, A1, 982270 & FR, B1, 2162093	1 - 15
Y	JP, A, 50-14987 (Hitachi, Ltd.) 17 February 1975 (17. 02. 75)	6, 7
Y	JP, U, 56-168802 (Hitachi, Ltd.) 14 December 1981 (14. 12. 81)	13
^a Special categories of cited documents: ¹⁵ "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "g" document member of the same patent family		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search ²		Date of Mailing of this International Search Report ²
August 9, 1984 (09. 08. 84)		August 20, 1984 (20. 08. 84)
International Searching Authority ¹		Signature of Authorized Officer ²⁰
Japanese Patent Office		

国 際 調 査 報 告

国際出願番号PCT/JP 8 4 / 0 0 2 5 1

I. 発明の属する分野の分類		
国際特許分類 (IPC) Int.Cl ⁸ G05B 9/03, G06F 11/18		
II. 国際調査を行った分野		
調 査 を 行 っ た 最 小 限 資 料		
分 類 体 系	分 類 記 号	
I P C	G05B 7/00-7/02, G05B 9/00-9/03, G05B 23/00-23/02, G06F 11/18	
最小限資料以外の資料で調査を行ったもの		
日本国実用新案公報 1926-1984年 日本国公開実用新案公報 1971-1984年		
III. 関連する技術に関する文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	請求の範囲の番号
Y	JP, A, 58-37702 (株式会社日立製作所) 3.5月.1983 (03.05.83)	1-15
Y	JP, A, 48-61886 (株式会社日立製作所) 29.8月.1973 (29.08.73) & DE, B2, 2258917 & CA, A1, 982270 & FR, B1, 2162093	1-15
Y	JP, A, 50-14987 (株式会社日立製作所) 17.2月.1975 (17.02.75)	6, 7
Y	JP, U, 56-168802 (株式会社日立製作所) 14.12月.1981 (14.12.81)	13
*引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 先行文献ではあるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献 「T」 国際出願日又は優先日の後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリーの文献		
IV. 認 証		
国際調査を完了した日 09.08.84	国際調査報告の発送日 20.08.84	
国際調査機関 日本国特許庁 (ISA/JP)	権限のある職員 特許庁審査官 長 沢 俊 一 郎	5 H 6 8 4 6